To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

1. **PURPOSE:** This directive provides TSA policy and procedures for requesting privileged access account creation, modification, or removal on a TSA information technology (IT) asset.

2. **SCOPE:** This directive applies to all TSA employees and contractors with access to the TSA network and/or IT assets.

3. **AUTHORITIES:**

   A. DHS *National Security Systems Policy* 4300B

   B. DHS *National Security Systems Handbook* 4300B

   C. DHS *Sensitive Systems Policy Directive* 4300A

   D. DHS *Sensitive Systems Policy Handbook* 4300A

   E. NIST Special Publication 800-37- *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

   F. NIST Special Publication 800-42- *Guidelines on Network Security Testing*

   G. NIST Special Publication 800-53- *Recommended Security Controls for Federal Information Systems and Organizations*

   H. TSA MD 1400.3, *Information Technology Security*

   I. TSA MD 1400.3, *Information Technology Security Handbook*

   J. TSA MD 200.7, *Records Management Program*

4. **DEFINITIONS:**

   A. Applicant: TSA employee or contractor who requires the creation, modification or removal of privileged access to a TSA IT asset. Applicants are users or administrators of TSA systems.

   B. Applicant Supervisor: TSA employee or contractor with oversight to determine the need for the Applicant's privileged access.

C. Authorization Official (AO): TSA official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to the agency. The AO has the final authority over privileged access accounts.

D. Chief Information Security Officer (CISO): TSA official assigned oversight responsibility for information security on all TSA networks, including management of the privileged access of TSA IT systems, applications, and tools on behalf of the AO.

E. Data Interactive Account: A type of account used for system data analysis.

F. Data Non-interactive Account: A type of account used for troubleshooting or monitoring of inherent system properties that is not intended for system data analysis.

G. Information System Security Officer (ISSO): TSA individual responsible for information security on an assigned set of systems or locations.

H. Privileged Access Account: An information system account with rights that enable a user to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, staff performing computing account administration, or other employees whose job duties require special privileges over a computing system or network. Privileged access applies to systems, tools, and applications that allow accounts with elevated permissions. Types of privileged access accounts include standard privileged access accounts, temporary privileged accounts, and service accounts.

NOTE: A privileged access account for which a waiver/exception has been approved to allow sharing of its credential (ID/password) may be referred to as shared privileged access account. For the purpose of this process, this differentiation is not made.

I. Privileged Access Rights: Account settings and elevated permissions that enable a user to take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users.

J. Service Account: Account that enables machine to machine or system to system communication.

K. System Owner (SO): TSA official responsible for the overall procurement, development, integration, modification, operation, maintenance and IT security of an information system.

L. Temporary Privileged Access Account: A privileged account with a pre-determined limited lifetime.

M. TSA IT Asset: Any IT component owned and operated by the TSA, including assets located at non-TSA facilities and non-TSA owned assets hosting TSA data. TSA IT Assets include, but are not limited to, workstations, laptop computers, infrastructure devices (switches, routers, firewalls, etc.), software (individual and enterprise), firmware, peripheral devices (USB drives, USB microphones, keyboards, etc.), personal electronic devices (PEDs), and mobile electronic media (MEM). These requirements shall extend to TSA assets located at non-TSA facilities.

5. RESPONSIBILITIES:

A. The Applicant is responsible for accurately completing and signing TSA Form 1429, *Privileged Access Request* for privileged access account creation, modification or removal to TSA IT assets as directed by the Applicant Supervisor.

B. The Applicant Supervisor is responsible for:

(1) Determining the need for the privileged access account.

(2) Submitting the request for privileged access account creation, modification or removal for TSA IT assets through the specified routing process.

C. The CISO is responsible for:

(1) Overseeing the requests for TSA IT systems, applications, and tools.

(2) Consolidating and reviewing monthly reports of privileged access accounts.

(3) Reviewing, approving, or denying privileged access requests when delegated by the AO.

D. The ISSO is responsible for:

(1) Reviewing, tracking and maintaining accurate records of privileged access accounts for their systems on behalf of the System Owner.

(2) Validating the privileged access rights of system users on an annual basis.

(3) Reporting the list of privileged access users to the CISO on a monthly basis.

(4) Ensuring proper actions are taken to remove privileged accounts, as needed.

(5) Retaining privileged access requests in accordance with the mandated records retention requirements.

E. The SO is responsible for:

(1) Overseeing all privileged access account requests for assigned systems, applications, and tools.

(2) Reviewing, approving or denying privileged access requests for their systems.

(3) Initiating privileged access account creation, modification or removal.

(4) Providing notification to the Applicant Supervisors on the status of the requests.

F. The AO is responsible for:

(1) Providing final approval over privileged access accounts to TSA systems.

(2) Reviewing monthly consolidated reports of privileged access accounts.

6. POLICY:

A. The SO shall ensure the creation and modification of all privileged access accounts for their systems upon requested approval.

B. Shared privileged access accounts shall not be permitted without an approved waiver or exception.

C. Approved requests for TSA temporary privileged access shall be valid for up to ninety (90) days from the date the request is approved. A new request shall be submitted by the Applicant Supervisor every ninety (90) days when temporary privileged access is required.

D. Accurate records of privileged access accounts shall be maintained for each system.

E. Reports of privileged access accounts for each system shall be generated and reviewed monthly.

F. Privileged access account removal requests shall be promptly submitted and processed for users no longer requiring access.

G. The AO may designate and delegate final approval over privileged access accounts to the CISO.

H. The CISO may designate and delegate review of each privileged access request to the Deputy CISO.

7. PROCEDURES:

A. Applicants requesting privileged access, service accounts, and/or temporary privileged access to TSA IT assets shall complete and submit TSA Form 1429 to their supervisor.

B. Applicants shall refer to and follow the OIT Standard Operating Procedure, *Privileged Access* for detailed instructions on submitting privileged access requests.

8. APPROVAL AND EFFECTIVE DATE: This policy is approved and effective the date of signature unless otherwise specified.

APPROVAL

Signed January 6, 2012

Dr. Emma Garrison-Alexander
Assistant Administrator for Information Technology/
Chief Information Officer

Date

EFFECTIVE

_____
Date

Distribution: All TSA Employees and Contract personnel
Point-of-Contact: Assistant Director Compliance & Policy, TSAIADPolicy@tsa.dhs.gov